WHAT IS CLAIMED IS:

1. A method for securing communications in a currency-handling machine comprising:

generating an encrypted transaction message based on a transaction event originating from the bill acceptor;

communicating the encrypted transaction message from the bill acceptor to a transaction controller over a communication channel;

decrypting the encrypted transaction message within the transaction controller; and

enabling the bill acceptor to accept a bill if the decrypted transaction message is authenticated.

2. The method of claim 1 wherein generating the encrypted transaction message includes applying an exclusive-or operation on at least one of a transaction message, a master-key, and a certification-key.

3. The method of claim 2 wherein the master-key is a predetermined value originating from the bill acceptor and communicated from the bill acceptor to the transaction controller over the communication channel during the initialization phase.

4. The method of claim 2 wherein the certification-key is a random value periodically communicated from the transaction controller to the bill acceptor over the communication channel.

5. The method of claim 1 wherein decrypting the transaction message includes decrypting the encrypted transaction message by applying an exclusive-or operation on at least one of an encrypted transaction message, a master-key, and a certification-key.

6. The method of claim 5 wherein decrypting the transaction message further includes checking the checksum of the encrypted transaction message.

7. The method of claim 6 further comprising disabling the bill acceptor if the result of the checksum fails.

8. The method of claim 6 further comprising sending an acknowledgement message if the result of the checksum passes.

9. The method of claim 1 wherein generating the encrypted transaction message includes applying to the transaction a modulus-based operation and using a private-key known only to the bill acceptor and a certification-key received during a previous communication with the transaction controller.

10. The method of claim 1 wherein decrypting includes applying to the encrypted transaction message a modulus-based operation and using a public key communicated from the bill acceptor to the transaction controller, wherein the result of the operation is an authentication value used to authenticate the source of the encrypted transaction message.

11. The method of claim 10 wherein decrypting further comprises applying a further modulus-based operation on the authentication value using the public-key and the certification-key, wherein the result of the operation is a data value used to evaluate the encrypted transaction message.

12. A method of securely installing a bill acceptor in a currency-handling machine comprising:

connecting a bill acceptor to a transaction controller;

enabling a secured setup mode to operate in the bill acceptor;

transmitting a master-key code from the bill acceptor to the transaction controller;

processing the master-key code in the transaction controller and generating a certification-key; and

transmitting the certification-key to the bill-acceptor to enable the bill-acceptor to operate.

13. A method of operating a currency-handling machine in a secure environment comprising:

generating an escrow message in response to an insertion of a bill into a bill acceptor;

encrypting the escrow message using a secured communication protocol, wherein the escrow message is formatted based on information derived from the bill;

communicating the encrypted escrow message from the bill acceptor to the transaction controller;

decrypting the escrow message using a secured communication protocol;

verifying the integrity of an escrow checksum of the decrypted escrow message;

sending a stack command to the bill acceptor, wherein the stack command includes a new certification-key, if the result of an escrow checksum reveals an authorized bill acceptor;

storing the bill and acknowledging the stack command by sending an encrypted stack message to the transaction controller;

receiving the stack message into the transaction controller;

decrypting the stack message using a secured communication protocol;

verifying the integrity of a stack checksum of the decrypted stack message; and

sending a credit command to the bill acceptor, wherein the credit command includes a new certification-key, if the result of the checksum reveals an authorized bill acceptor.

14. A method of claim 13 further comprising generating a warning and disabling the bill acceptor if the result of at least one of the escrow checksum and the stack checksum reveals an unauthorized bill acceptor.

15. A method of securing communications between a transaction controller within a currency-handling machine and a bill acceptor comprising:

requesting a master-key from the bill acceptor during the setup process;

transmitting a certification-key to the bill acceptor during the setup process;

generating a formatted transaction message based on an event originating at the bill acceptor;

retrieving the certification-key and the master-key at the bill acceptor;

generating an encrypted transaction message based on a exclusive-or operation on at least one of the master-key and the certification-key at the bill acceptor;

receiving the encrypted transaction message;

decrypting the encrypted transaction message based on the exclusive-or operation on at least one of the master-key and the certification-key; and

verifying and taking an appropriate action based on the integrity of the checksum of the result of decrypting the encrypted transaction message.

16. A method of securing communications between a transaction controller within a currency-handling machine and a bill acceptor comprising:

transmitting a certification-key to the bill acceptor during the setup process;

generating a public-key and a private-key within the bill acceptor;

receiving the public-key from the bill acceptor;

generating an encrypted transaction message based on the private-key and the certification-key at the bill acceptor;

decrypting the encrypted transaction message based on the public-key; and

verifying the authenticity of the encrypted transaction message using the certification-key.

17. A method of securing communications between a transaction controller within a currency-handling machine and a bill acceptor comprising:

generating a certification-key at the bill acceptor during the setup process, wherein the certification-key is generated by a pseudo-random-generator with an initial seed value;

receiving the initial seed value from the bill acceptor during the setup process;

generating a certification-key during the setup process, wherein the certification-key is generated by a pseudo-random-generator with an initial seed value received from the bill acceptor;

generating an encrypted transaction message at the bill acceptor based on the certification-key;

decrypting the encrypted transaction message based on the certification-key, where the certification-key is generated by a pseudo-random-generator at the transaction controller; and

verifying the authenticity of the encrypted transaction message by comparing the certification-key generated by the pseudo-random-generator in the transaction controller with the certification-key obtained from encrypted transaction message.

18. The method of 17 wherein a certification-key is subsequently generated at the bill acceptor when a subsequent transaction message is encrypted, and a certification-key is subsequently generated at the transaction controller when the subsequent transaction message is decrypted.

19. A method of securing communications between a transaction controller within a currency-handling machine and a bill acceptor comprising:

generating at the bill acceptor a current-key and a future-key during the setup process;

receiving the future-key during the setup process;

storing the future-key during the setup process;

generating at the bill acceptor an encrypted transaction message based on the current-key and the future-key;

decrypting the encrypted transaction message based on the future-key, where the future-key is retrieved from the previously stored future-key; and

verifying the authenticity of the encrypted transaction message by comparing the future-key which was previously obtained and retrieved from the transaction controller with the current-key obtained from the encrypted transaction message.

20. The method of claim 19 wherein decrypting includes obtaining from the encrypted transaction message a future-key and storing the future-key at the transaction controller to be used when decrypting a subsequent transaction message containing a current-key and a new future-key, and wherein the current-key obtained from the subsequent decrypted transaction message is to be compared with the future-key previously stored at the transaction controller.

21. A secure bill handling apparatus comprising:

a bill acceptor including a processor and memory for authenticating bills and generating and encrypting data; and

a transaction controller connected to the bill acceptor, wherein the transaction controller is associated with the currency-handling machine, and wherein the transaction controller includes a processor and memory for decrypting and authenticating data received by the bill acceptor, and responding to the bill acceptor based on the result of the authenticity of the data received from the bill acceptor.

22. The apparatus of claim 21 wherein the bill acceptor encrypts the transaction message based on the exclusive-or operation using a master-key and a certification-key, and wherein the transaction controller decrypts the encrypted transaction message based on the exclusive-or operation using the master-key and the certification-key.

23. The apparatus of claim 21 wherein the bill acceptor encrypts the transaction message based on a private-key and a certification-key, and wherein the transaction controller decrypts the encrypted transaction message based on the public-key.

24. A method for securing communications in a currency-handling machine comprising:

generating an encrypted transaction message based on a transaction event;

communicating the encrypted transaction message from a bill acceptor to a transaction controller over a communication channel;

decrypting the encrypted transaction message; and

enabling the bill acceptor to accept a bill if the decrypted transaction message is authenticated.

25. The method of claim 24 wherein generating the encrypted transaction message includes applying an exclusive-or operation on at least one of a transaction message, a master-key, and a certification-key.

26. The method of claim 25 wherein the master-key is a predetermined value, and the certification-key is a random.

27. The method of claim 24 wherein decrypting the transaction message includes decrypting the encrypted transaction message by applying an exclusive-or operation on at least one of an encrypted transaction message, a master-key, and a certification-key.

28. The method of claim 27 wherein decrypting the transaction message further includes checking a checksum of the encrypted transaction message.

29. The method of claim 28 further comprising at least one of disabling the bill acceptor if the result of the checksum fails, and sending an acknowledgement message if the result of the checksum passes.

30. The method of claim 24 wherein generating the encrypted transaction message includes applying to the transaction a modulus-based operation using a private-key and a certification-key that was received during a previous communication.

31. The method of claim 24 wherein decrypting includes applying to the encrypted transaction message a modulus-based operation using a public key and wherein the result of the operation is an authentication value used to authenticate the source of the encrypted transaction message.

32. The method of claim 31 wherein decrypting further comprises applying a further modulus-based operation on the authentication value using the public-key and a certification-key, wherein the result of the operation is a data value used to evaluate the encrypted transaction message.